

Automating Barrier Assessment with Mobile Security Robots

Daniel Carroll, Doriann Jaffee (CSC), Katherine Mullens

Space and Naval Warfare Systems Center San Diego (SSC San Diego)

Code 2371, 53406 Woodward Road, San Diego, CA 92152-7383

619-553-7636, FAX: 619-553-6188, Daniel.Carroll@navy.mil, <http://www.spawar.navy.mil/robots/>

Computer Sciences Corporation (CSC), San Diego, CA

ABSTRACT

Barrier assessment is the time consuming and labor-intensive process of manual inspection of locks on doors and gates by security guards. The Mobile Detection Assessment Response System (MDARS) uses Unmanned Ground Vehicles (UGVs) and a Barrier Assessment System (BAS) to automate lock inspection and report an unsecured area to the security force thereby improving their ability to detect and respond to unauthorized access.

MDARS is a joint U.S. Army-Navy development effort to field mobile robots at Department of Defense (DoD) sites for physical security and automated inventory missions. MDARS UGVs patrol autonomously outside of storage facilities and operate payloads for intruder detection, inventory assessment, and barrier assessment. For barrier assessment, the robots remotely monitor the status of locks with Internal Locking Devices. The robot will notify the user if a lock is opened or has been compromised.

This paper details the evolution of the BAS from prototype design to successfully passing developmental testing. Additional emphasis is placed on integration of the barrier assessment payload with the MDARS Exterior robot, installation of the BAS support equipment in a storage area, user interface, and overall system improvements at an MDARS operational site.

1. Standard Operating Procedures (SOP) for Physical Security

The responsibilities for security forces at Department of Defense (DoD) sites include:

- 1) Securing entrances,
- 2) Patrolling accessible areas,
- 3) Monitoring security alarm system on a 24-hour basis,
- 4) Performing physical security checks on inaccessible areas,
- 5) Investigating unauthorized intrusions, and
- 6) Responding to alarm situations.

Security forces at DoD storage sites also protect sensitive and valuable assets. Typically small to medium sized assets (e.g., munitions) are stored in locked bunkers while larger assets (e.g., armored personnel carriers) are stored externally in an area that may be enclosed by security fences and gates.

A site's SOP defines the scope and responsibilities for the security force. For example, certain bunkers, also called igloos, with a "high security padlock" may need to be inspected as often as once every 24 hours. SOPs may require the guard to go to the bunker and physically "shake" the padlock to ensure it is

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE SEP 2003		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Automating Barrier Assessment With Mobile Security Robots				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Daniel /Carroll; Katherine /Mullens				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Space and Naval Warfare Systems Center Code 2371 53406 Woodward Road San Diego, CA 92152-7383				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 11	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

secure. Some of the larger US Army depots have thousands of bunkers stretched over hundreds of miles of access roads.

Under current operations, such a site requires a significant amount of patrolling and checking by the security guard force. This is a labor-intensive task since their personnel need to drive to each bunker, step out of their vehicle, inspect the lock, and record activity in a logbook. Each lock check takes several minutes and is a monotonous task. In addition, personnel are required to perform manual inventory checks on the contents of each bunker as often as once every six months. This is a major endeavor.

2. Concept of Operations

The goal of the Mobile Detection Assessment Response System (MDARS) is to field autonomous vehicles for security and inventory assessment functions at DoD warehouses and storage sites. The program is managed by the Office of the Product Manager, Physical Security Equipment, (PM-PSE) at Ft. Belvoir, VA, with the Space and Naval Warfare Systems Center San Diego (SSC San Diego) providing technical direction and systems integration functions.

Having MDARS installed at a DoD site changes the security picture dramatically, as shown in **Figure 1**. In this case, Unmanned Ground Vehicles (UGVs) patrol the site; a guard supervisor commands and controls the UGVs from a central control station. The supervisor has mobile guard unit(s) available to investigate reported alarms and suspicious events.

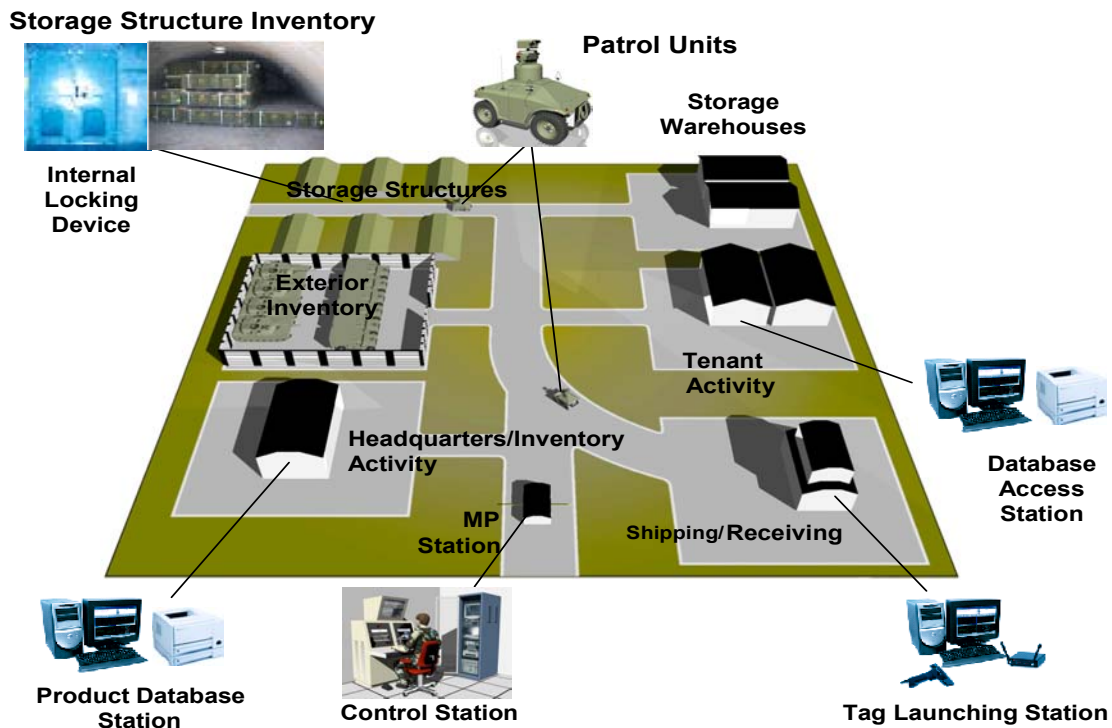


Figure 1. Overview of Typical Site with MDARS

Bunkers are secured with high security Internal Locking Devices (ILDs) that are magnetically instrumented to detect whether the lock is open or closed. These locks are remotely monitored by the UGVs, with the guard supervisor being notified at the central console if a lock is open or has been compromised. **Figure 2** shows the Internal Locking Device (ILD).

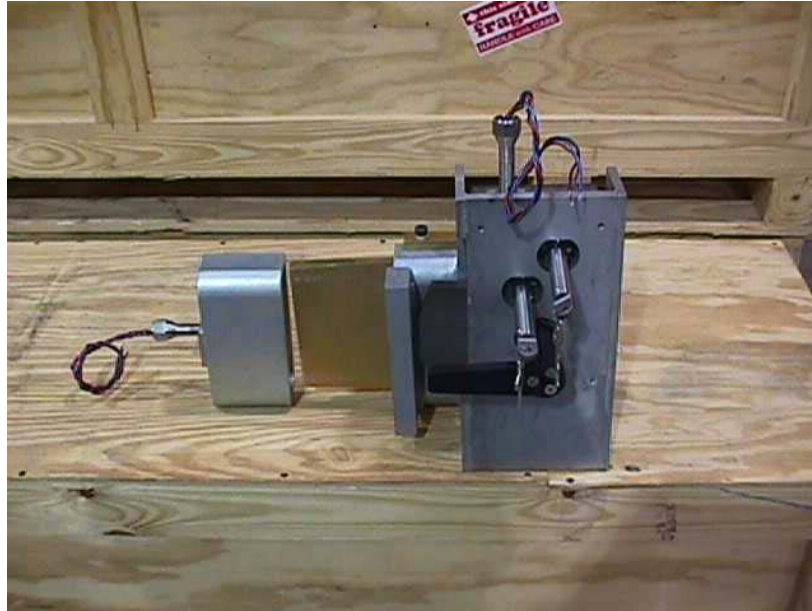


Figure 2. Internal Locking Device (ILD)

Critical, sensitive, or high-value assets have radio frequency identification (RFID) tags attached to them. In the course of their patrols, UGVs collect the IDs of these tags. The Multiple Resource Hosts Architecture (MRHA) software monitors the presence and location of the tags, and provides reports indicating whether any tags are missing, not in their assigned locations, tampered with, or have low batteries. When problems are reported, personnel can send a UGV to conduct an inventory of a given bunker and/or use a handheld tag reader to check for the presence of specific tagged item(s). **Figure 3** shows an RFID tag and handheld reader. The RFID tag is approximately the size of a small box of matches.



Figure 3. Radio Frequency Identification (RFID) Tag and Handheld Reader

In this scenario, UGVs each have an assigned mission. Each vehicle patrols several hours per day (or night), traversing its assigned area checking for possible intruders, monitoring the status of locks, and checking on the presence and location of RFID-tagged items.

While patrolling a site, UGVs generally travel on paved or gravel roads. Gates through which they pass are equipped with network-enabled devices allowing them to be opened and closed remotely by the central system.

The MDARS system is intended to handle normal operations automatically, notifying the guard supervisor only when some unusual condition occurs. If a UGV detects an open lock, for example, the MRHA will raise an alarm at the central console and will await action from the guard supervisor. The guard supervisor can then assess the situation and, if necessary, send a patrol to investigate. If an MDARS vehicle encounters an obstacle, on the other hand, it will use its obstacle avoidance sensors and onboard software to maneuver around the obstacle and continue its mission. Only if it encounters something that totally blocks its path, such as a washed-out road, will it stop and notify the guard supervisor.

Because the MDARS vehicles conduct their missions autonomously, a site achieves a high level of security with very little of the routine patrolling, lock checking and inventory checking generally required of the guard force. This frees up guards to investigate problem situations identified by MDARS.

3. Technical Evidence

General Dynamics Robotic Systems (GDRS) (formerly Robotic Systems Technology (RST)), was awarded an MDARS Broad Agency Announcement (BAA) contract in 1993 for the development of the outdoor UGVs. The mobility base is a rugged four-wheel hydrostatic-drive diesel-powered vehicle equipped with active-laser, ultrasonic-sonar, millimeter-wave-radar, and stereovision sensors for collision avoidance, and differential global positioning system (DGPS) for autonomous navigation. MDARS passed a Technical Feasibility Test (TFT) in May 2000, and a System Development and Demonstration (SDD) contract was awarded to GDRS in January 2002. An Early User Appraisal (EUA) for the MDARS System is scheduled for FY04 at Hawthorne Army Depot, NV. **Figure 4** depicts the MDARS BAA and SDD Vehicles.

The MDARS command and control console is based upon the SSC San Diego's MRHA, a distributed processing system that allows coordinated control of multiple autonomous resources, including up to 255 unmanned vehicles, remote fixed sensors, and/or unmanned sensor pods. **Figure 5** shows the MDARS console in the Robotic Operations Command Center (ROCC) at SSC San Diego.

The MDARS payloads pertaining to physical security currently consist of a barrier assessment system to check the status of high-security locks on bunkers, a radio frequency identification (RFID) tag and reader system to perform product assessment (inventory), and an intrusion detection sensor (IDS) suite. The barrier assessment system consists of electronic Internal Locking Devices (ILDs) installed in bunker doors, as well as special-purpose computers to monitor the locks. UGVs collect the state of each lock during their patrols and transmit the information to the central console where an alarm is raised if a

lock is open. RFID tags affixed to critical, sensitive, or high-dollar items are read by tag readers attached to bunkers as well as mounted on UGVs; tag data is collected by UGVs as part of their normal patrol duty, and the data is used by the MRHA to update the locations of the tagged items in addition to verifying their presence. The IDS systems currently use motion detection techniques with a variety of sensor modalities to decrease the frequency of false alarms while maintaining a high probability of detection. IDS will not be discussed further here. Most of the payload components are based on commercial off-the-shelf (COTS) equipment.



Figure 4. MDARS BAA and SDD Vehicles



Figure 5. Robotic Operations Command Center (ROCC)

3.1 Barrier Assessment System (BAS)

The BAS performs automatic sensing of the state of instrumented locks on bunker doors within a patrol area, thus providing a way for security personnel to determine if controlled areas are secured without having to manually check every lock in the patrol area. A conceptual diagram of BAS operation is shown in **Figure 6**.

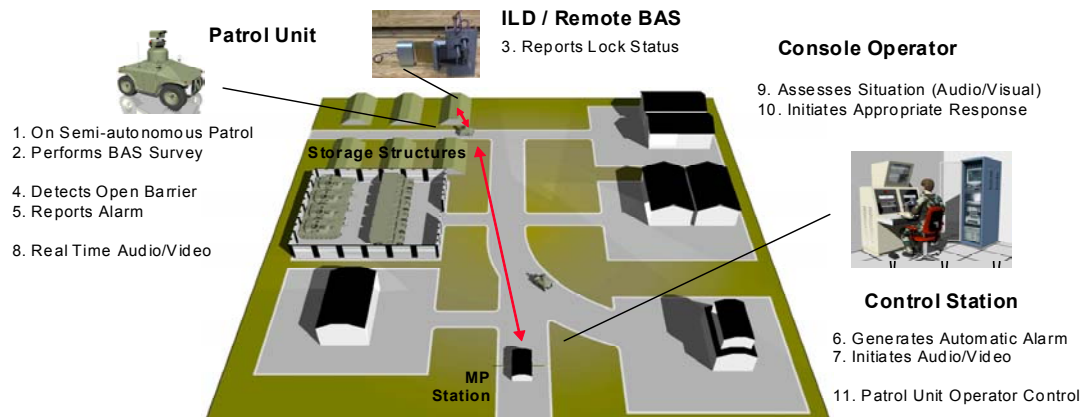


Figure 6. Overview of BAS Operation

An ILD attached to each bunker door is magnetically instrumented to detect whether the lock is open or closed. Magnetic sensors raise signals on the appropriate wires when the lock is in the open or the closed position. These wires are connected to the store-and-forward computer attached to the bunker. Besides maintaining the current state of the lock, the store-and-forward computer maintains a count of the number of times the lock has been opened and closed as well as the date/time of the last times the lock was opened and closed.

An MDARS vehicle will stop within 100 meters of the bunker and upload the state of the lock (“open” or “closed”) from the store-and-forward computer; if the lock can’t be read it will assign a state of “error”. The UGV also uploads the count of the number of times the lock has been opened/closed as well as the timestamp of the most recent opening and closing events. The vehicle then passes this information to the MRHA. The MDARS console displays icons depicting the most recent status of locks, and if a lock is detected to be open, the user is notified by a visual and audio alarm. To assist in an investigation, the guard supervisor has the additional information on when the lock was most recently opened and closed as well as the count of how many times the lock was opened and closed. **Figure 7** shows a lock alarm being displayed at the central console.

3.2 Asset Tracking

Asset (or inventory) tracking is performed by the Product Assessment System (PAS). In order to monitor the locations of high-value, controlled, or special-interest assets in the inventory, RFID tags are attached to the products. Each tag broadcasts a signal at a constant rate (called a “chirp rate”). These signals contain the tag’s unique ID as well as a tamper alarm if the tag has been removed from the item to which it was mounted, a low battery alarm to indicate if the battery is near the end of its life, and a counter which increments if the tag is moved.

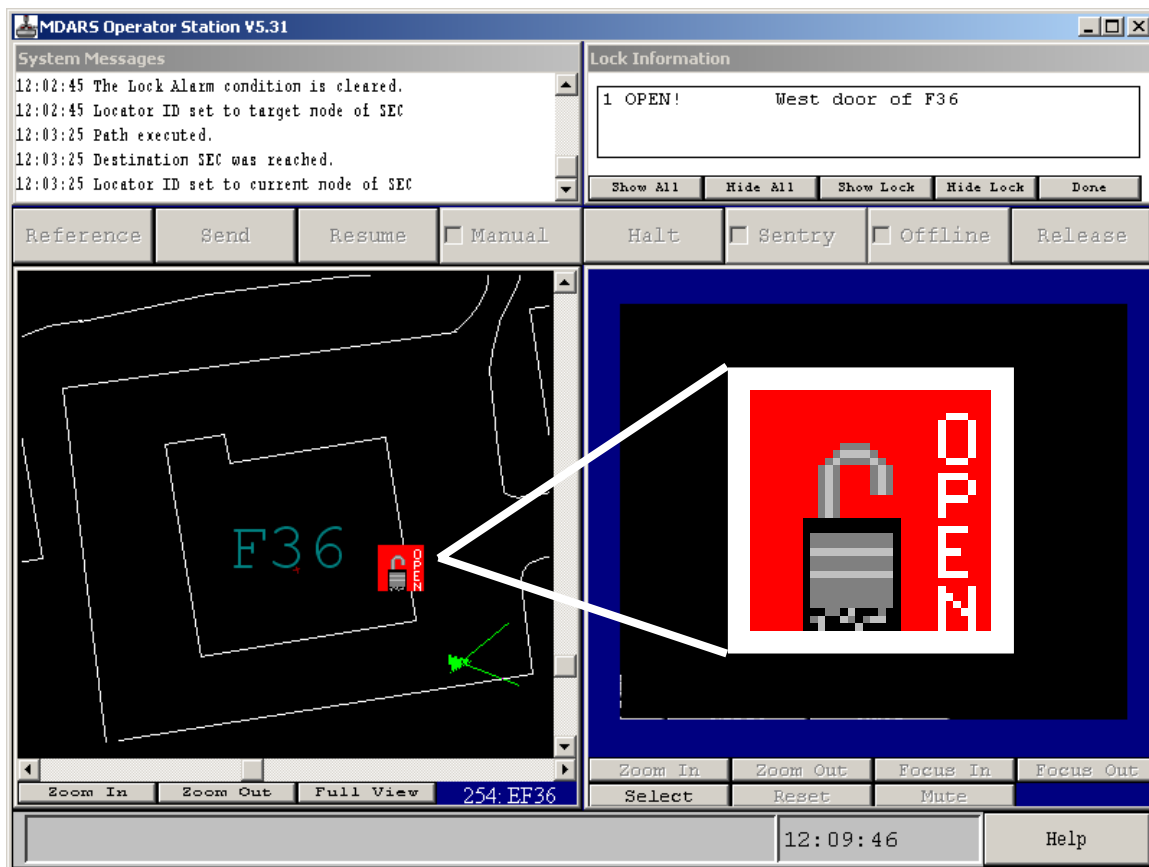


Figure 7. Lock Alarm Displayed on Console (with Lock Open Icon in Inset)

Each bunker containing tagged assets is outfitted with an RFID tag reader and a store-and-forward computer, both installed in a weatherproof enclosure external to the bunker. Inside the bunker are antennas that receive signals from the RFID tags and transmit them to the tag reader. The reader passes the tag data to the store-and-forward computer, which retains the tag data until the next time a UGV requests it. When stopped near a bunker, a UGV will read both lock data (as described above) and tag data during the same stop.

RFID tags attached to assets stored externally are read by a tag reader onboard a UGV. At regular stops during its patrol, each vehicle activates its onboard tag reader to read any tags within its range. The vehicle uploads the location at which it stops and a list of tags read at that location to the MRHA on the MDARS console. The MRHA PAS computers automatically transfer the data from the MDARS console and triangulate an approximate location based upon multiple tag reads. The MRHA PAS maintains an inventory database and produces reports to inform warehouse personnel of any problems such as missing or moved inventory. MDARS PAS payloads use *Mantis* RFID tags and tag readers manufactured by RF Code.

The information on RFID-tagged items is stored in a database, from which personnel can request reports at any time. Most of these are exception reports, alerting personnel to items that are missing, tags that have been tampered with, items not in their assigned locations, or other unusual conditions. Once alerted to apparently missing or misplaced item(s), personnel can investigate further by either sending a UGV to

perform an inventory operation (i.e., read tags) at a given location or else by using a handheld RFID tag reader at the location in question to determine whether a tagged item is present. The automated asset tracking provided by MDARS gives site personnel far more timely information than the manual inventory counts they've had in the past.

4. Evolutionary Development

The MDARS program employs evolutionary development using iterative “design-build-test” cycles. The goal of each cycle is to improve and to optimize the existing system. Cycles are typically linked to a major milestone in the acquisition model and have intermediate cycles to “lock-in” functionality. The “design” phase typically begins with rapid-prototyping for concept demonstration; the “build” phase involves refining the design and carrying out changes to the baseline system; the “test” phase requires systems integration testing. The recent “design-build-test” cycles for the MDARS programs have concentrated on improvements made in order to meet or exceed the user requirements. The cycles concluded with the testing conducted for MDARS TFT.

4.1 Prototype

Both the vehicles and the MRHA were modified to support the system development for MDARS TFT. On the vehicles, components and algorithms on the navigation, obstacle avoidance, communications, and payloads subsystems were upgraded and optimized. For the entire system, an MRHA Interface Design Document (IDD) was implemented to facilitate communications; multiple analog audio and video links were replaced by a seamless digital link; and a Network-Enabled Resource Device (NERD) was designed to interface remote devices, such as gates, to the MRHA.

The MRHA IDD defines the communications between the MDARS command and control console and remote resources, such as MDARS vehicles, unmanned sensors, etc. The IDD defines common protocols and messages for wireless communications for all resources. Prior to implementation of the IDD, each vehicle had its own vendor-specific protocol and controller. Implementation of the IDD allowed the vehicles not only to be controlled from a single console, but also to reuse legacy software developed for mobility and for payloads.

4.2 Integration Testing

The MDARS TFT was conducted in May 2000 by the U.S. Army Aberdeen Test Center (ATC) in the Edgewood Area of Aberdeen Proving Ground (APG), MD. TFT was conducted to characterize the performance of the MDARS system for safety, navigation, obstacle avoidance, command and control, communications, and payloads.

For the BAS test, an ILD was installed on a bunker door and was connected to two RFID tags that were used to monitor whether the lock was open or closed. One tag was active and regularly “chirping” its ID if the lock was closed, while the other tag was active if the lock was open. **Figure 8** shows the installation of the ILD on the bunker door. A tag reader was placed within the bunker to read the RFID tags attached to the lock as well as other RFID tags attached to products within the bunker. The reader was cabled to a radio whose antenna was attached to the outside of the bunker.

The MDARS robotic vehicle was sent by the testers to six positions ranging from 25 feet to 100 feet from the bunker door. **Figure 9** shows the bunker and the positions (labeled A – F) at which the vehicle stopped. Some of these positions were within line-of-sight to the door while others (position A in particular) were blocked by a large concrete and earthen barrier. Four iterations of this test were conducted. The results of the test were that the status of the lock was read correctly every time from every vehicle position.

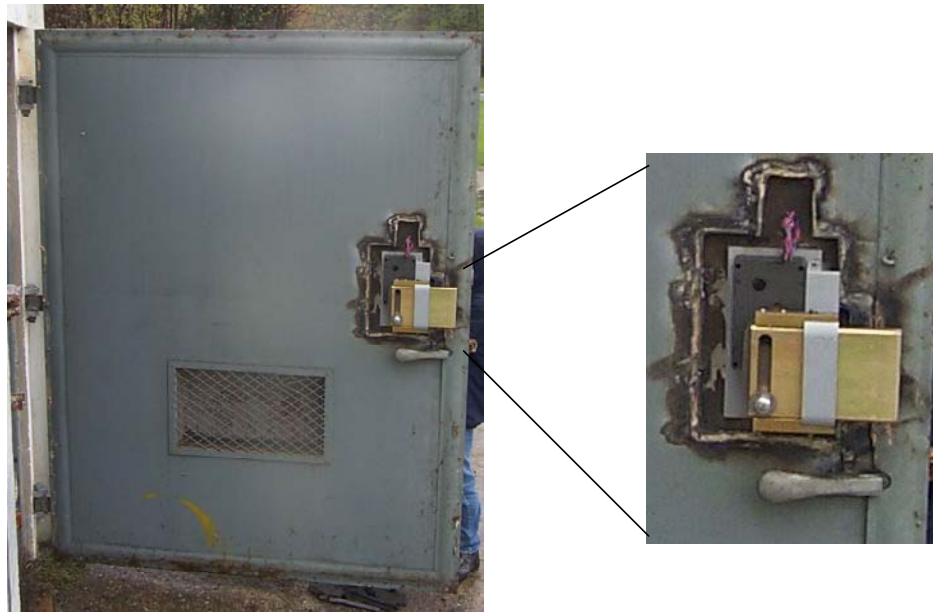


Figure 8. ILD Installed on Bunker Door

4.3 Recommended Enhancements

Based upon feedback from the operational users and testers, below is a partial list of enhancements for the MDARS payloads for physical security:

Tag Attachment: Further research needs to be done by industry to develop a standard method to attach RFID tags to a variety of products and surfaces.

Lock-Only Bunker: It may be required to monitor the lock on a bunker that doesn't contain RFID-tagged assets. A cost-savings alternative to attaching a store-and-forward computer to such a bunker is to use RFID tags to monitor the state of the lock. One or more tags would be connected to the ILD and these tags would transmit the state of the lock to a tag reader onboard a UGV.

Alarm on Missing Critical Assets: Currently RFID-tagged assets are noted as Missing only when a person requests a PAS database report. Assets that are considered critical could be monitored more closely and an alarm raised if a UGV has passed within range of such an asset (either stored in a bunker or stored externally) and has not read the tag attached to the asset.

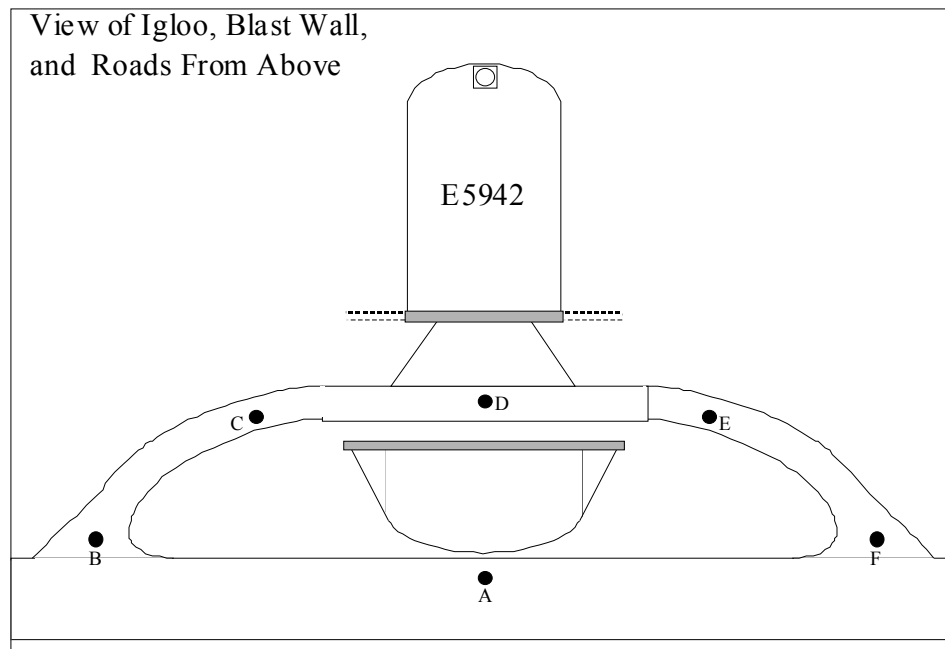


Figure 9. Overhead Diagram of Access Road between Bunker and Blast Wall with Lock Reading Locations

5. Conclusion

The MDARS Barrier Assessment System is one component of a fully automated physical security and force protection system using unmanned vehicles and sensors. It provides automated monitoring of high security locks, and relieves humans of the time-consuming job of checking locks manually. Besides providing current lock state and alerting the user if a lock is open, it provides additional information in the form of date/time when the lock was last opened and closed, as well as a count of lock openings and closings. MDARS uses a combination of payloads for intruder detection as well as RFID inventory of high-value assets. MDARS provides sites with improved security, frees personnel from performing tedious manual jobs, and allows personnel to concentrate on responding to high priority threats.

6. References

- Carroll, D., Gilbreath, G.A., and H.R. Everett, "Extending Mobile Security Robots to Force Protection Missions," AUVSI Unmanned Systems 2002, Lake Buena Vista, FL, July 9-11, 2002
- Everett, H.R. and D.W. Gage, "From Laboratory to Warehouse: Security Robots Meet the Real World," *International Journal of Robotics Research*, Special Issue on Field and Service Robotics, volume 18, number 7, July 1999, pp. 760-768.
- Heath-Pastore, T.A., H.R. Everett, and K. Bonner, "Mobile Robots for Outdoor Security Applications", American Nuclear Society 8th International Topical Meeting on Robotics and Remote Systems (ANS'99), Pittsburgh, PA, 25-29 April 1999.

VanSeeters, C.A., "Abbreviated Test Report for the Technical Feasibility Test (TFT) of the Mobile Detection Assessment Response System - Exterior (MDARS-E)," Report No. ATC-8287, US Army Aberdeen Test Center, Aberdeen Proving Ground, MD, 21005-5059, July 2000.